

Indian Banks Data Breach 2016

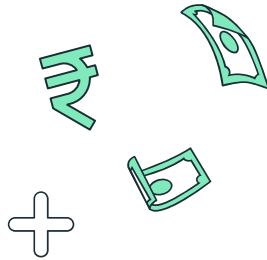
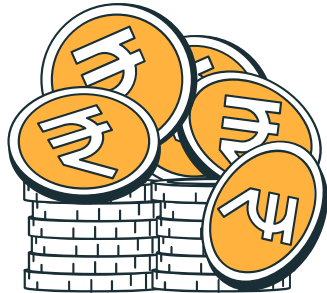
Incident Overview, Impact & Lessons

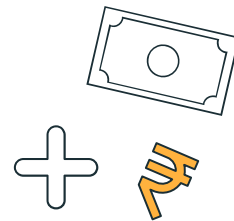
20230802289

20230802325

20230802288

20230802380





The Attack Breakdown

01

WHO?

Major Indian banks including SBI, HDFC, ICICI, YES Bank, and Axis Bank.

Third-party vendor: Hitachi Payment Systems.

02

What? (Incident)

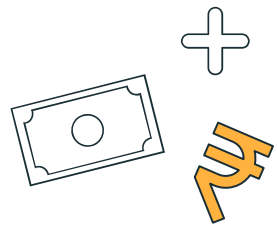
3.2 million debit cards compromised.

Fraudulent use detected outside India (China and US).

Hitachi Payment Systems:

- A third-party payment and ATM transaction processor operating ATM and Point-of-Sale (POS) networks for several Indian banks.
- Managed backend switching infrastructure for ATM/POS transactions; banks relied on Hitachi's systems to process card transactions securely.





The Attack Breakdown

HOW? - The Attack Method

03

- Attackers targeted a Hitachi-powered ATM, reportedly starting with a Yes Bank ATM.
- Method: Malware (malicious software) was inserted into Hitachi's ATM switching network.
- The malware harvested card magnetic stripe data and PINs as customers made ATM/POS transactions.
- With this stolen data, attackers cloned cards and used them for unauthorized withdrawals overseas.
- Root Cause: Security lapses included lack of strong network segmentation and poor database/password protection on archival transaction data.



Impact & Analysis

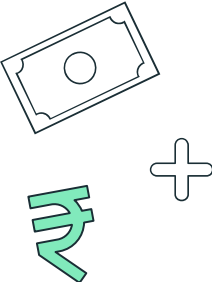
0 CUSTOMER IMPACT:

- 3.2 million cards at risk; nearly 600,000 replaced by SBI alone.
- Widespread card blocks, affecting banking operations.

0 FINANCIAL IMPACT:

- Large-scale unauthorized withdrawals; significant bank losses (exact figure not made public for this breach.)





Security Analysis



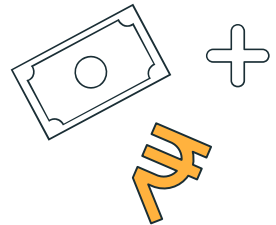
Failure in monitoring
and malware
detection at vendor
level.

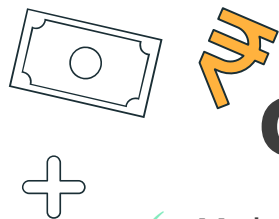


Attack leveraged
centralized third-
party infrastructure
(Hitachi),
compromising
multiple banks
connected to the
network.

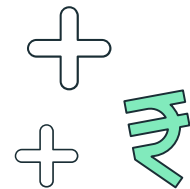


Poor database
security (e.g., missing
passwords, archival
access).





Case Resolution: How was it solved?



- ✓ Multiple banks noticed international card fraud on cards still in India; forensic audits initiated.
- ✓ Banks blocked compromised cards and issued replacements.
- ✓ Hitachi's systems were isolated, malware removed after a full security audit.

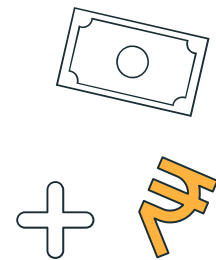
Post-Breach Actions:

- ✓ Full-scale audit by SISA Information Security.
- ✓ Enhanced malware detection and network segmentation steps implemented.
- ✓ RBI mandated security assessments for all banks





Lessons Learned & Mitigation



01

Strengthen third-party vendor risk management and oversight.

02

Mandatory malware detection, network segmentation, and regular forensic assessments.

03

Implement robust real-time monitoring, incident response, and network segmentation.

04

Enforce stricter authentication and secure storage of sensitive banking data.

05

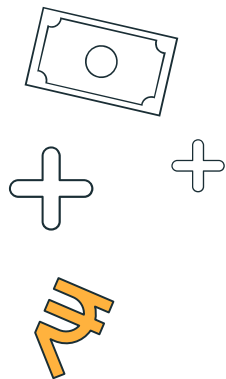
Implement chip-based (EMV) cards and upgrade legacy infrastructure.

06

Regularly update and patch ATM/payment infrastructure and educate banking staff.



Conclusions



2016 breach exposed critical gaps in third-party payment system security within Indian banking.

Prompt detection and improved controls reinforced cyber resilience in banking.

Industry-wide awareness and collaboration remain vital to combat future threats.

Continuous vigilance is necessary as cyber threats evolve.

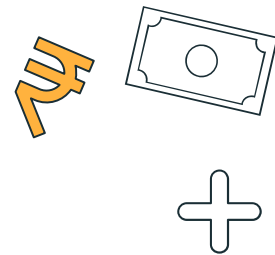
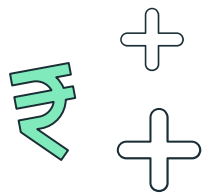




References

- ❑ **Data Privacy and Protection - IJERT**
- ❑ **Wikipedia: 2016 Indian bank data breach**
- ❑ **Kenes Exhibitions:**
HDFC, ICICI Bank, Axis Bank, SBI & Yes Bank Hit With Data Breach
- ❑ **Indian Express:**
Multiple banks hit, 3.2 million debit cards compromised, how it happened, what happens now
- ❑ **Reserve Bank of India (RBI) Notice -**
Cybersecurity Incident in Cards
- ❑ **Press Release:**
Data Breach in Banks with respect to Cards, Ministry of Finance





Thank You!

